

By Cont. Subst. concl. D

a meter for metering the packets belonging to the application group; and  
a user interface that allows a user to specify the assigned portion of the bandwidth.--

### REMARKS

By this amendment, claims 3, 5, 8, 9, 12, 14, 17 and 18 have been amended. Currently, claims 1, 3-10, and 12-18 are pending in this application.

#### Rejection under 35 U.S.C. 102(e)

Claims 1, 3-10, and 12-18 were rejected under 35 U.S.C. 102(e) as anticipated by Ma (U.S. Patent No. 5,953,338). This rejection is respectfully traversed in view of the following arguments.

Ma discloses a system for allocating bandwidth between clients on an ATM network to guarantee each client receives the level of service specified in its contract agreement (see col. 7, lines 39-53, and Fig. 8). Specifically, when a client wishes to access the ATM network, the system control module, which is connected to at least one of the ATM switches on the network, determines whether the requested virtual connections can be created in the network. (Abstract). To do this, the call admission control checks the client's total traffic against the client's contract agreement. (see Fig. 8). Accordingly, Ma teaches a system for allocating bandwidth on the ATM backbone of the network, so that each client is assured the amount of bandwidth for which it has paid.

Ma does not teach or suggest how a client should go about allocating the bandwidth between internal applications. Specifically, Ma states (col. 8, lines 5-6), "Clients of the virtual private network are ... responsible for prioritizing their own calls." (Col. 8, lines 5-6).

This application is directed to this technical area not described by Ma – how can virtual private networks prioritize their own calls. As discussed in the application as originally filed, for example at page 4, bandwidth management is achieved by a server 100 connected to router 120. A bandwidth management process is implemented on the server 100 that allows the server to police bandwidth utilization on its associated links that are vulnerable to congestion. These links generally include the server's access links to the ISP circuits, and the LAN links on the server's site. (page 4, lines 9-25).

The Examiner has taken the position that Ma teaches a server (citing Call Control 140 and col. 7, lines 5-14) and has taken the position that the server is a VPN server (citing Fig. 1A, col. 5, lines 57-66). Applicants respectfully submit that the Call Control 140 is not a VPN server, as that term is used in this application.

The Call Control 140 in Ma “handles the majority, if not all, of the call requests for virtual private network 170.” It “implements an overall, network-wide call admission strategy, which determines whether to admit or reject a request to allow a virtual connection to be setup.” (col. 7, lines 5-8). The “call control module 140 handles specific client requests for a call requiring access to virtual private network 170 (in Fig. 1A). Using a procedure to implement a call admission strategy procedure, ... centralized call admission control/usage monitor module 145 handles a request for permission to access virtual private network 170 that was received by call control module 140.” (col. 7, lines 12-19). Thus, the Call Control 140 in Ma is a process that runs on the network and communicates with the routers to implement service level agreements on the network.

A VPN server, as that term is used in the instant application, is a server that manages VPN services for the client to enable one LAN to communicate with another LAN over a public

network. Specifically, applicants state at page 1, lines 14-15, "VPN servers employ a tunneling technique that enables one network to send its data to a destination via another network." Applicants further explain, at page 2, lines 16-17, that a VPN server, as used in this application, is a server "which authenticates, encapsulates, and de-encapsulates the packets."

Thus, the Call Control 140 is not a VPN server, as that term is used in this application, since it does not employ a tunneling technique that enables one network to send its data to a destination via another network. E.g., it does not perform encapsulation or encryption to enable packets to be securely transmitted over an untrusted network.

Applicants recognize that claim terms during examination will be interpreted as broadly as their terms reasonably allow. MPEP 2111.01 (8<sup>th</sup> Ed. p. 2100-47). However, where the applicant has provided a clear definition in the specification, the claims are to be interpreted according to that definition. Id. In this instance, applicant has clearly used the term "VPN server" as referring to a server that authenticates, encapsulates, and de-encapsulates the packets. (p. 2, lines 16-17). Accordingly, applicant respectfully submits that, pursuant to MPEP 2111.01, the Examiner must afford the claimed "VPN server" the definition ascribed to it in the specification.

Independent claims 1 and 10 recite "wherein the server is a VPN server." Since Ma fails to teach or suggest a VPN server as that term is used in this application, applicants respectfully request that the rejection under 35 U.S.C. 102(e) of independent claims 1 and 10 be withdrawn.

Independent claims 3, 5, 8, 9, 12, 14, 17, and 18 have all been amended to refer to a VPN server. Accordingly, applicants respectfully submit that these claims are patentable over Ma and respectfully request that the rejection under 35 U.S.C. 102(e) be withdrawn.

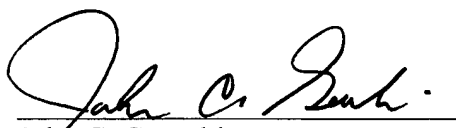
Reply Dated October 25, 2002  
Serial No. 09/740,052

Conclusion

In view of foregoing claim amendments and remarks, it is respectfully submitted that the application is now in condition for allowance and an action to this effect is respectfully requested. If there are any questions or concerns regarding the amendments or these remarks, the Examiner is requested to telephone the undersigned at the telephone number listed below.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-13361).

Respectfully Submitted

  
John C. Gorecki  
Registration No. 38,471

Dated: October 25, 2002

John C. Gorecki, Esq.  
Patent Attorney  
165 Harvard St.  
Newton, MA 02460  
Tel: (617) 796-9024  
Fax: (617) 795-0888

**VERSION WITH MARKINGS TO SHOW CHANGES MADE**

Submitted herewith is a marked-up version of the amended claims to show changes made in the foregoing Amendment.

**IN THE CLAIMS**

Claims 3, 5, 8, 9, 12, 14, 17 and 18 have been amended as follows:

-- 3. (Twice Amended) A method for a VPN server that manages bandwidth of a remote link, comprising:

assigning a portion of the bandwidth to at least one application group; and

metering packets belonging to the application group;

wherein the server is directly connected to other links having larger bandwidth than the available bandwidth of the remote link.--

--5. (Twice Amended) A method for a VPN server that manages bandwidth of a remote link, comprising:

assigning a portion of the bandwidth to at least one application group; and

metering packets belonging to the application group;

wherein the packets belonging to the application group contend equally for the portion of the bandwidth.--

--8. (Twice Amended) A method for a VPN server that manages bandwidth of a remote link, comprising:

assigning a portion of the bandwidth to at least one application group;

metering packets belonging to the application group; and

allowing a user to specify the bandwidth of the remote link from a user interface.--

--9. (Twice Amended) A method for a VPN server that manages bandwidth of a remote link, comprising:

assigning a portion of the bandwidth to at least one application group;

metering packets belonging to the application group; and

allowing a user to specify the portion of the assigned bandwidth from a user interface.--

--12. (Twice Amended) A system for managing bandwidth of a remote link comprising:

a VPN server

a contention pool having a portion of the bandwidth for at least one application group;

and

a meter for metering the packets belonging to the application group;

wherein the server is directly connected to other links having larger bandwidth than the available bandwidth of the remote link.--

--14. (Twice Amended) A system for managing bandwidth of a remote link comprising:

a VPN server

a contention pool having a portion of the bandwidth for at least one application group;

and

a meter for metering the packets belonging to the application group;

wherein the packets belonging to the application group contend equally for the contention pool.--

--17. (Twice Amended) A system for managing bandwidth of a remote link comprising:  
a VPN server  
a contention pool having a portion of the bandwidth for at least one application group;  
and  
a meter for metering the packets belonging to the application group; and  
a user interface that allows a user to specify the bandwidth of the link.--

--18. (Twice Amended) A system for managing bandwidth of a remote link comprising:  
a VPN server  
a contention pool having a portion of the bandwidth for at least one application group;  
and  
a meter for metering the packets belonging to the application group; and  
a user interface that allows a user to specify the assigned portion of the bandwidth.--